[APPLICATION] Sharing trusted hardware across multiple operational environments
US Pat. 10804489 - Filed Mar 18, 2004
In one embodiment, these requests may take the form of **TPM** commands as described in the **TPM** Main Specification, Part 3, version 1.2. A **VMM TPM** multiplexer **...**

[APPLICATION] Enabling platform network stack control in a virtualization platform
US Pat. 10954905 - Filed Sep 30, 2004
Thus, a **VMM** will launch only if the key in memory matches the hash. If a virus maliciously modifies the **VMM**, **TPM** will not allow the **VMM** to launch because **...**

[APPLICATION] Platform configuration apparatus, systems, and methods
US Pat. 11396266 - Filed Mar 31, 2006
The guest 108 may, for example, issue a request 131 to the **TPM** 114 to use the PCR set 112 located at **TPM** port 132. The **VMM** 116 may intercept the request 131 **...**

Method and system to support a trusted set of operational environments using ...
US Pat. 7222062 - Filed Dec 23, 2003 - Intel Corporation
VMM 115 operates to coordinate execution of VM sessions 130. In one embodiment, **VMM** 115 **....** In one embodiment, **VMM** 115 multiplexes various **TPM** commands or **...**

[APPLICATION] Platform configuration register virtualization apparatus, systems, and methods
US Pat. 11095034 - Filed Mar 31, 2005
The guest 108 may, for example, issue a request 131 to the **TPM** 114 to use the PCR set 112 located at **TPM** port 132. The **VMM** 116 may intercept **...**

[APPLICATION] Method and apparatus for providing secure virtualization of a trusted ...
US Pat. 10876994 - Filed Jun 24, 2004
VMM 106 may use a standard process for creating AIKs to create CK 56. Virtual **TPM** service 104 may subsequently use CK 56 when certifying virtual **...**

[APPLICATION] Methods and arrangements to launch trusted, co-existing environments
US Pat. 11527180 - Filed Sep 26, 2006

Partition manager 159 or 180 may authenticate **VMM** 136 via **TPM** 190 and receive a key from **TPM** 190 to decrypt data 132 and processes 134. **...**

[**APPLICATION**] Local secure service partitions for operating system security
US Pat. 11097697 - Filed Apr 1, 2005
In particular, the audit software 24 is modified to call an audit log service in partition 18 using a partition ID provided by hypervisor or **VMM** 12 from **TPM ...**

[**APPLICATION**] Method and System for Implementing a Mobile Trusted Platform Module
US Pat. 11840823 - Filed Aug 17, 2007 - Fujitsu Limited
Some of these components, such as **TPM** device 2110 and interface 2120 are **...**
[0033] Virtual machine monitor 2130 (**VMM** 2130) may be a software program, **...**

[**APPLICATION**] Low cost trusted platform
US Pat. 11170597 - Filed Jun 28, 2005
Consequently, a **TPM** may be emulated in the STM, allowing a coequal privilege access level to **...** a virtual monitor may be a virtual machine monitor (**VMM**). **...**

Stay up to date on these results using the patents RSS feed on **VMM TPM**.

Gooooogle ▶
Result Page: 1 2 3 4 **Next**